

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 1 1 - 8 5 5 0 4

(43) 公開日 平成 1 1 年 (1 9 9 9) 3 月 3 0 日

(51) Int. Cl. °	識別記号	庁内整理番号	F I	技術表示箇所
G06F 9/06	550		G06F 9/06	550 Z
13/00	351		13/00	351 Z
G09C 1/00	630		G09C 1/00	630 B
	640			640 D
	660			660 D

審査請求 未請求 請求項の数 6 O L (全 1 6 頁)

(21) 出願番号 特願平 9 - 2 4 6 7 5 2

(22) 出願日 平成 9 年 (1 9 9 7) 9 月 1 1 日

(71) 出願人 0 0 0 0 0 6 0 1 3

三菱電機株式会社

東京都千代田区丸の内二丁目 2 番 3 号

(72) 発明者 宮崎 一哉

東京都千代田区丸の内二丁目 2 番 3 号 三

菱電機株式会社内

(72) 発明者 中嶋 春光

東京都千代田区丸の内二丁目 2 番 3 号 三

菱電機株式会社内

(72) 発明者 中川路 哲男

東京都千代田区丸の内二丁目 2 番 3 号 三

菱電機株式会社内

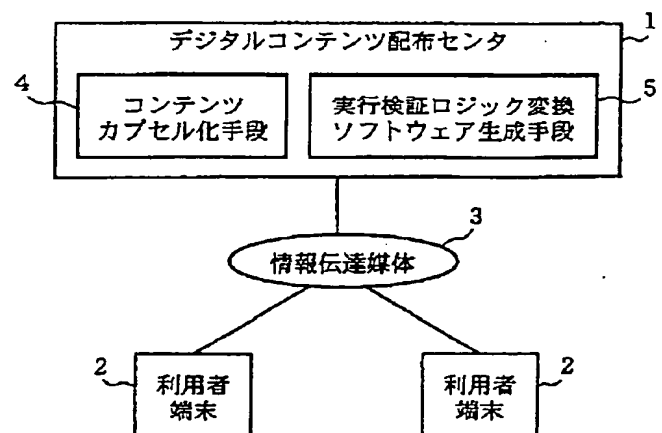
(74) 代理人 弁理士 田澤 博昭 (外 1 名)

(54) 【発明の名称】 デジタルコンテンツ配布システム装置

(57) 【要約】

【課題】 要求に応じた使用制限を柔軟に指定してコンテンツの試使用版を生成できないという課題があった。

【解決手段】 コンテンツの検証と実行制御を行うロジックである第 1 の実行検証ロジックを生成して前記コンテンツに結合する。また前記コンテンツの検証と実行制御を行う第 2 の実行検証ロジックを生成し、前記コンテンツに結合された前記第 1 の実行検証ロジックを前記第 2 の実行検証ロジックに置き換えて結合し直す実行検証ロジック変換手段を持つ実行検証ロジック変換ソフトウェアを生成する。そして、前記第 1 の実行検証ロジックの結合されたコンテンツと前記実行検証ロジック変換ソフトウェアを利用者端末に提供する。



4 : コンテンツカプセル化手段 (結合手段)

5 : 実行検証ロジック変換ソフトウェア生成手段
(変換ソフトウェア生成手段)

【特許請求の範囲】

【請求項 1】 デジタルコンテンツを配布するデジタルコンテンツ配布センタと、前記デジタルコンテンツの提供を受ける一つあるいは複数の利用者端末と、前記デジタルコンテンツ配布センタと前記利用者端末との間を接続する情報伝達媒体で構成されるデジタルコンテンツ配布システム装置において、

前記デジタルコンテンツ配布センタは、

デジタルコンテンツの検証と実行制御を行うロジックである第 1 の実行検証ロジックを生成し、生成した第 1 の実行検証ロジックを前記デジタルコンテンツに結合する結合手段と、

前記デジタルコンテンツの検証と実行制御を行う第 2 の実行検証ロジックを生成し、該生成した前記第 2 の実行検証ロジックへ前記デジタルコンテンツに結合された前記第 1 の実行検証ロジックを置き換えて結合し直して実行検証ロジック変換ソフトウェアを生成する変換ソフトウェア生成手段とを具備し、

前記第 1 の実行検証ロジックを結合されたデジタルコンテンツと前記実行検証ロジック変換ソフトウェアを、前記情報伝達媒体を経由して前記利用者端末に提供することを特徴とするデジタルコンテンツ配布システム装置。

【請求項 2】 デジタルコンテンツを制作する制作者端末と、

制作者に代わり当該制作者の制作した前記デジタルコンテンツの著作権管理の代行を行う著作権管理代行センタと、

前記デジタルコンテンツの配布を行うデジタルコンテンツ配布センタと、

前記デジタルコンテンツの提供を受ける利用者端末と、前記制作者端末と前記著作権管理代行センタと前記デジタルコンテンツ配布センタと前記利用者端末とを接続する情報伝達媒体を備え、

前記デジタルコンテンツの制作者端末は、

前記デジタルコンテンツの検証と実行制御を行うロジックである第 1 の実行検証ロジックを生成し、生成した第 1 の実行検証ロジックを前記デジタルコンテンツに結合する結合手段を具備し、

前記著作権管理代行センタは、前記デジタルコンテンツ配布センタから送られた実行検証ロジックの仕様を反映して第 2 の実行検証ロジックを生成し、該生成した前記第 2 の実行検証ロジックへ前記第 1 の実行検証ロジックを置き換えて実行検証ロジック変換ソフトウェアを生成する変換ソフトウェア生成手段を具備し、

前記デジタルコンテンツ配布センタは、

前記実行検証ロジックの仕様を生成する仕様生成手段と、

前記著作権管理代行センタから送られた前記実行検証ロジック変換ソフトウェアに含まれた前記第 2 の実行検証ロジックと前記デジタルコンテンツ配布センタにおいて

生成された前記実行検証ロジックの仕様とを比較検証する比較検証手段とを具備し、前記第 1 の実行検証ロジックを結合されたデジタルコンテンツと前記変換ソフトウェア生成手段により生成された実行検証ロジック変換ソフトウェアを、前記情報伝達媒体を経由して前記利用者端末に対し提供することを特徴とするデジタルコンテンツ配布システム装置。

【請求項 3】 結合手段は、

デジタルコンテンツの一部あるいは全部を暗号化するためのコンテンツ鍵を生成するコンテンツ鍵生成手段と、該コンテンツ鍵生成手段により生成した前記コンテンツ鍵により前記デジタルコンテンツの一部あるいは全部を暗号化するコンテンツ暗号化手段と、

電子透かしにより前記デジタルコンテンツに情報を不可分の形で組み込む電子透かし組込手段と、

前記デジタルコンテンツの電子署名を生成する電子署名生成手段と、

前記実行検証ロジックのハッシュ値をメッセージ識別子として生成する識別子生成手段と、

前記コンテンツ暗号化手段により一部あるいは全部に暗号化を施され、前記電子透かし組込手段により電子透かしを施されたデジタルコンテンツと前記電子署名生成手段により生成した前記電子署名と前記実行検証ロジックと前記識別子生成手段により生成したメッセージ識別子を結合するコンテンツ結合手段とを具備し、

変換ソフトウェア生成手段は、

前記コンテンツ暗号化手段により暗号化を施された前記デジタルコンテンツの前記メッセージ識別子と前記コンテンツ鍵を関連付けて管理する暗号化コンテンツ管理手段と、

デジタルコンテンツ配布センタから送られた実行検証ロジックの仕様を反映して第 2 の実行検証ロジックを生成する第 2 の実行検証ロジック生成手段を具備し、

第 1 の実行検証ロジックを前記第 2 の実行検証ロジック生成手段で生成された前記第 2 の実行検証ロジックに置き換える実行検証ロジック変換ソフトウェアを生成し、前記第 2 の実行検証ロジックは、

前記デジタルコンテンツの電子署名を検証する電子署名検証手段と、

前記メッセージ識別子を検証する識別子検証手段と、

前記コンテンツ鍵を格納するコンテンツ鍵格納手段と、

該コンテンツ鍵格納手段に前記コンテンツ鍵が格納されているか否かを判断するコンテンツ鍵格納判定手段と、

前記コンテンツ鍵が格納されている場合に当該コンテンツ鍵で暗号化されているデジタルコンテンツを復号する復号手段とを具備することを特徴とする請求項 1 または請求項 2 記載のデジタルコンテンツ配布システム装置。

【請求項 4】 コンテンツ鍵格納手段は、デジタルコンテンツの配布対象となる利用者の公開鍵でコンテンツ鍵を暗号化して格納する暗号化コンテンツ鍵格納手段を具

備し、

復号手段は、前記暗号化コンテンツ鍵格納手段により格納されている前記コンテンツ鍵を前記利用者の秘密鍵で復号し、コンテンツ暗号化手段により暗号化されているデジタルコンテンツを前記復号されたコンテンツ鍵で復号することを特徴とする請求項 3 記載のデジタルコンテンツ配布システム装置。

【請求項 5】 実行検証ロジック変換ソフトウェアは、利用者情報を電子透かしによりデジタルコンテンツに埋め込む利用者情報埋込手段を備えていることを特徴とする請求項 1 または請求項 2 記載のデジタルコンテンツ配布システム装置。

【請求項 6】 実行検証ロジック変換ソフトウェアは、第 1 の実行検証ロジックが第 2 の実行検証ロジックへ変換される際にデジタルコンテンツ配布センタへ情報伝達媒体を介して課金情報を送付して提供する課金情報提供手段を備えていることを特徴とする請求項 1 または請求項 2 記載のデジタルコンテンツ配布システム装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、インターネット等のオープンな広域ネットワーク上でデジタルコンテンツを販売するデジタルコンテンツ配布システム装置に関し、特に販売したデジタルコンテンツの著作権管理、課金管理、不正利用の防止を実現できるデジタルコンテンツ配布システム装置に関するものである。

【0002】

【従来の技術】 図 16 は、例えば特開平 8 - 6 7 8 4 号公報に示された従来のデジタルコンテンツ配布システム装置のブロック図を示しており、図において、101 は利用者用の端末装置、102 は利用制御手段、103 は施錠／破壊処理手段、104 はソフトウェア／著作物の製品、105 は継続利用要求処理手段、106 は開錠／再利用処理手段、107 は配布者（販売者）の管理装置、108 は利用者情報管理手段、109 は資格審査処理手段、110 は利用権利更新処理手段である。

【0003】 次に動作について説明する。購入した利用者の端末装置 101 に、施錠／破壊処理手段 103 の組み込まれているソフトウェア／著作物の製品 104 と鍵を通信回線経由で送る。端末装置 101 では、送られてきた前記鍵を用いて購入したソフトウェアなどを開錠して使用する。有効期限がくればソフトウェアまたは著作物は自動的に施錠または破壊されて作動を停止する。利用者が継続利用要求処理手段 105 により管理装置 107 に対して更新を要求すると、資格審査処理手段 109 が利用者情報管理手段 108 の内容を参照し、問題がなければ利用権利更新処理手段 110 が、新しい鍵または製品を通信回線経由で端末装置 101 に送る。端末装置 101 では送られてきた前記鍵または製品を受け、開錠／再利用処理手段 106 により開錠して次の有効期限ま

で購入したソフトウェアまた著作物の利用を継続する。

【0004】

【発明が解決しようとする課題】 従来のデジタルコンテンツ配布システム装置は以上のように構成されているので、期間のみでなく利用できる機能範囲や参照可能なデータの範囲など要求に応じた使用制限を柔軟に指定してコンテンツの試使用版を生成できないという課題があった。

【0005】 また、従来のデジタルコンテンツ配布システム装置は、制作者の立場からの配慮が欠けており、制作者による著作権管理、配布者による課金管理をそれぞれ容易に行うことができる構成や処理の流れになっていないという課題があった。

【0006】 さらに、従来のデジタルコンテンツ配布システム装置は、配布者がデジタルコンテンツの暗号化鍵の管理を行うため、制作者は配布者に著作物の管理を全面的に頼らなければならないという課題があった。

【0007】 さらに、従来のデジタルコンテンツ配布システム装置は、利用者情報のデジタルコンテンツへの埋め込みを考慮していないか、あるいは利用者情報の埋め込みが利用者自身の意志に委ねられるという課題があった。

【0008】 さらに、従来のデジタルコンテンツ配布システム装置は、課金のタイミングがデジタルコンテンツの提供時あるいは復号鍵の提供時であり、利用者の受け取り否認が生じ易いという課題があった。

【0009】 この発明は上記のような課題を解決するためになされたもので、使用条件や利用範囲などを柔軟に設定できる試使用版コンテンツを設定できるデジタルコンテンツ配布システム装置を得ることを目的とする。

【0010】 また、この発明は著作権代行センタを想定した構成にして、制作者に大きな負担を要求せずに権利保護が実現できるデジタルコンテンツ配布システム装置を得ることを目的とする。

【0011】 さらに、この発明は電子透かし、電子署名、暗号化、実行検証ロジックの組み込みを煩雑な手続きを必要とせずに行えるデジタルコンテンツ配布システム装置を得ることを目的とする。

【0012】 さらに、この発明は配布者にコンテンツの鍵を知られにくいデジタルコンテンツ配布システム装置を得ることを目的とする。

【0013】 さらに、この発明は煩雑な手続きを必要とせずに正確な利用者情報をコンテンツに不可分な形で埋め込み不正コピーや不正な配布を抑止しやすいデジタルコンテンツ配布システム装置を得ることを目的とする。

【0014】 さらに、この発明は実際にデジタルコンテンツを利用可能にする処理を利用者が実施する際に配布者が課金情報を取得できるデジタルコンテンツ配布システム装置を得ることを目的とする。

【0015】

【課題を解決するための手段】この発明に係るデジタルコンテンツ配布システム装置は、デジタルコンテンツの検証と実行制御を行うロジックである第1の実行検証ロジックを生成し、生成した第1の実行検証ロジックを前記デジタルコンテンツに結合する結合手段と、前記デジタルコンテンツの検証と実行制御を行う第2の実行検証ロジックを生成し、該生成した前記第2の実行検証ロジックへ前記デジタルコンテンツに結合された前記第1の実行検証ロジックを置き換えて結合し直して実行検証ロジック変換ソフトウェアを生成する変換ソフトウェア生成手段とを具備し、前記第1の実行検証ロジックを結合されたデジタルコンテンツと前記実行検証ロジック変換ソフトウェアを、前記情報伝達媒体を経由して前記利用者端末に提供するデジタルコンテンツ配布センタを備えるようにしたものである。

【0016】この発明に係るデジタルコンテンツ配布システム装置は、デジタルコンテンツの検証と実行制御を行うロジックである第1の実行検証ロジックを生成し、生成した第1の実行検証ロジックを前記デジタルコンテンツに結合する結合手段を具備した制作者端末と、デジタルコンテンツ配布センタから送られた実行検証ロジックの仕様を反映して第2の実行検証ロジックを生成し、該生成した前記第2の実行検証ロジックへ前記第1の実行検証ロジックを置き換えて実行検証ロジック変換ソフトウェアを生成する変換ソフトウェア生成手段を具備した著作権管理代行センタと、前記実行検証ロジックの仕様を生成する仕様生成手段と、前記著作権管理代行センタから送られた前記実行検証ロジック変換ソフトウェアに含まれた第2の実行検証ロジックと前記実行検証ロジックの仕様とを比較検証する比較検証手段とを具備し、前記第1の実行検証ロジックを結合されたデジタルコンテンツと前記実行検証ロジック変換ソフトウェアを情報伝達媒体を経由して利用者端末に対し提供するデジタルコンテンツ配布センタとを備えるようにしたものである。

【0017】この発明に係るデジタルコンテンツ配布システム装置は、コンテンツ暗号化手段により一部あるいは全部に暗号化を施され、電子透かし組込手段により電子透かしを施されたデジタルコンテンツと電子署名生成手段により生成した電子署名と実行検証ロジックと識別子生成手段により生成したメッセージ識別子とを結合するコンテンツ結合手段と、第1の実行検証ロジックを第2の実行検証ロジック生成手段で生成された第2の実行検証ロジックに置き換える実行検証ロジック変換ソフトウェアを生成する変換ソフトウェア生成手段とを備え、前記第2の実行検証ロジックが電子署名検証手段と識別子検証手段とコンテンツ鍵格納手段とコンテンツ鍵格納判定手段と復号手段とを備えるようにしたものである。

【0018】この発明に係るデジタルコンテンツ配布システム装置は、デジタルコンテンツの配布対象となる利

用者の公開鍵でコンテンツ鍵を暗号化して格納する暗号化コンテンツ鍵格納手段と、該暗号化コンテンツ鍵格納手段により格納されている前記コンテンツ鍵を前記利用者の秘密鍵で復号し、コンテンツ暗号化手段により暗号化されているデジタルコンテンツを前記復号されたコンテンツ鍵で復号する復号手段とを備えるようにしたものである。

【0019】この発明に係るデジタルコンテンツ配布システム装置は、利用者情報を電子透かしによりデジタルコンテンツに埋め込む利用者情報埋込手段を実行検証ロジック変換ソフトウェアが備えるようにしたものである。

【0020】この発明に係るデジタルコンテンツ配布システム装置は、第1の実行検証ロジックが第2の実行検証ロジックへ変換される際にデジタルコンテンツ配布センタへ情報伝達媒体を介して課金情報を送付して提供する課金情報提供手段を実行検証ロジック変換ソフトウェアが備えるようにしたものである。

【0021】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態1. 図1は、この発明の実施の形態1によるデジタルコンテンツ配布システム装置の全体構成を示すブロック図である。図1において、1はデジタルコンテンツを配布するデジタルコンテンツ配布センタ、2はデジタルコンテンツの提供を受けデジタルコンテンツを利用する利用者端末、3はデジタルコンテンツ配布センタ1と利用者端末2を接続し情報を伝達する情報伝達媒体、4は実行検証ロジックを生成し、これをデジタルコンテンツと結合するコンテンツカプセル化手段（結合手段）、5はカプセル化されたコンテンツの前記実行検証ロジックを新たに生成した実行検証ロジックに変換する実行検証ロジック変換手段を持つ実行検証ロジック変換ソフトウェアを生成する実行検証ロジック変換ソフトウェア生成手段（変換ソフトウェア生成手段）である。

【0022】図2はコンテンツカプセル化手段4が生成するデジタル化されたコンテンツを示すブロック図である。図2において、6はコンテンツカプセル化手段4が生成するカプセル化コンテンツ、7はデジタルコンテンツの実行制御や検証のための実行検証手段を提供する第1の実行検証ロジック、8はデジタル情報であるデジタルコンテンツを示す。

【0023】次に動作について説明する。図3は、この実施の形態1におけるデジタルコンテンツ配布システム装置の動作を示すフローチャートである。ステップST1は、デジタルコンテンツ配布センタ1においてコンテンツカプセル化手段4により第1の実行検証ロジック7を生成し、この生成した第1の実行検証ロジック7をデジタルコンテンツ8と結合してカプセル化コンテンツ6を生成するステップである。このステップST1では、

7

デジタルコンテンツ配布センタ 1 において、コンテンツカプセル化手段 4 を用いて第 1 の実行検証ロジック 7 を生成し、オーサリングツールなど他のツール等で、生成された既存のデジタルコンテンツ 8 と前記第 1 の実行検証ロジック 7 を結合してカプセル化コンテンツ 6 を生成する。

【 0 0 2 4 】ここでデジタルコンテンツ 8 は、例えばイメージ、動画、音声、テキスト、ソフトウェア、あるいはそれらの複合化されたものである。また、第 1 の実行検証ロジック 7 は、例えば、起動時の初期メッセージ表示、対象となるデジタルコンテンツ 8 の正当性検証、そしてユーザ ID、マシン ID、日時などの条件判断を行うことによって参照あるいは実行の制御を行うコードであり、デジタルコンテンツ 8 を操作するために用意されたプログラミングインタフェースを利用して記述される。条件判断は、第 1 の実行検証ロジック 7 に埋め込まれた値と実行時に得た値の比較演算により行っても良いし、あるいは両者の値のパターンのハッシュ値を比較するようにしても良い。

【 0 0 2 5 】次のステップ S T 2 は、前記ステップ S T 1 で生成したカプセル化コンテンツ 6 を情報伝達媒体 3 を介して利用者端末 2 に配布するステップであり、ステップ S T 1 で生成されたカプセル化コンテンツ 6 を、情報伝達媒体 3 を介してデジタルコンテンツ配布センタ 1 から利用者端末 2 に配布する。

【 0 0 2 6 】続くステップ S T 3 では、デジタルコンテンツ配布センタ 1 の実行検証ロジック変換ソフトウェア生成手段 5 により、第 2 の実行検証ロジックを生成してカプセル化コンテンツ 6 の第 1 の実行検証ロジック 7 を前記第 2 の実行検証ロジックに置き換える実行検証ロジック変換手段を持つ実行検証ロジック変換ソフトウェアを生成する。

【 0 0 2 7 】ステップ S T 4 では、前記ステップ S T 3 において生成した実行検証ロジック変換ソフトウェアを情報伝達媒体 3 を介してデジタルコンテンツ配布センタ 1 から利用者端末 2 に配布する。

【 0 0 2 8 】次のステップ S T 5 では、前記ステップ S T 4 で配布された実行検証ロジック変換ソフトウェアを、利用者端末 2 において前記ステップ S T 2 で配布されたカプセル化コンテンツ 6 に適用し、カプセル化コンテンツ 6 の第 1 の実行検証ロジック 7 を前記第 2 の実行検証ロジックに置き換える。

【 0 0 2 9 】なお、ステップ S T 2 とステップ S T 3 の順序は逆になっても良い。またステップ S T 2 とステップ S T 4 が同時に行われても良い。また、通常、第 1 の実行検証ロジック 7 を持つカプセル化コンテンツ 6 は試使用版として最初に利用者に配布しておく構成であってもよい。

【 0 0 3 0 】以上のように、この実施の形態 1 によれば、最初に第 1 の実行検証ロジック 7 をデジタルコンテ

8

ンツ 8 に結合してカプセル化コンテンツ 6 を生成し、後から第 2 の実行検証ロジックに置き換えるようにしているので、第 1 の実行検証ロジック 7 を伴うカプセル化コンテンツ 6 を、デジタルコンテンツの実行制限を設けた試使用版デジタルコンテンツとして配布し、利用者が購入要求をデジタルコンテンツ配布センタ 1 に送り、この購入要求に応じた代金を支払うことによって実行制限の緩い実行検証ロジックに置き換える実行検証ロジック変換ソフトウェアを配布し、利用者は送られてきた前記実行検証ロジック変換ソフトウェアを前記試使用版のカプセル化コンテンツ 6 に施すことにより実使用版のカプセル化コンテンツ 6 をインストールすることができ、デジタルコンテンツを利用可能にする処理を利用者が実施する際に配布者が課金情報を取得でき、課金に応じて配布者が前記デジタルコンテンツの利用を許可することのできる効果が得られる。

【 0 0 3 1 】また、使用を許可するための鍵を配布する構成と違い、実行検証ロジックを置き換える構成であるから、予め何を制限するかをデジタルコンテンツに埋め込んでおき、それを実施するか解除するかを切り換えるだけでなく、デジタルコンテンツの利用実行に対するより柔軟な制御を後付けで施すことができる効果が得られる。さらに、デジタルコンテンツは概して容量が大きいいため、試使用版デジタルコンテンツを CD-ROM やデジタル放送で配布し、容量の小さな実行検証ロジック変換ソフトウェアについては公衆回線を介して配布することができる効果が得られる。

【 0 0 3 2 】実施の形態 2. 前記実施の形態 1 は、デジタルコンテンツ配布センタ 1 がデジタルコンテンツのカプセル化や実行検証ロジック変換ソフトウェアの生成を行うようにしたものであるが、この実施の形態 2 のデジタルコンテンツ配布システム装置は、より制作者の著作権保護を実現し易くするものである。図 4 は、この発明の実施の形態 2 によるデジタルコンテンツ配布システム装置の全体構成を示すブロック図である。図 4 において図 1 と同一または相当の部分については同一符号を付し説明を省略する。図において、9 はデジタルコンテンツの制作者が利用する制作者端末、10 はデジタルコンテンツの制作者の著作権管理を代行する著作権管理代行センタ、11 は実行検証ロジック変換ソフトウェア生成手段 5 に対して与える第 2 の実行検証ロジックの仕様を生成する実行検証ロジック仕様生成手段（仕様生成手段）、12 は実行検証ロジック変換ソフトウェアの実行検証ロジックを検証する実行検証ロジック検証手段（比較検証手段）である。

【 0 0 3 3 】次に動作について説明する。図 5 は、このデジタルコンテンツ配布システム装置の動作を示すフローチャートである。ステップ S T 11 は、制作者端末 9 においてコンテンツカプセル化手段 4 で第 1 の実行検証ロジック 7 を持つカプセル化コンテンツ 6 を生成するス

10

20

30

40

50

テップである。このステップ S T 1 1 では、制作者端末 9 のコンテンツカプセル化手段 4 で第 1 の実行検証ロジック 7 を生成し、デジタルコンテンツ 8 と結合することによりカプセル化コンテンツ 6 を生成する。

【 0 0 3 4 】 次のステップ S T 1 2 は、ステップ S T 1 1 で生成したカプセル化コンテンツ 6 を情報伝達媒体 3 を介して利用者端末 2 に配布するステップである。このステップ S T 1 2 では、ステップ S T 1 1 で生成したカプセル化コンテンツ 6 を情報伝達媒体 3 を介して利用者
10 端末 2 に配布するが、ここで生成したカプセル化コンテンツ 6 の配布は制作者端末 9 が行ってもよいし、一旦、著作権管理代行センタ 1 0 を経由し、あるいはデジタルコンテンツ配布センタ 1 を経由して行っても良い。また、公衆回線を使って行っても良いし、C D - R O M あるいはデジタル放送を介して行っても良い。

【 0 0 3 5 】 続くステップ S T 1 3 は、デジタルコンテンツ配布センタ 1 の実行検証ロジック仕様生成手段 1 1 で第 2 の実行検証ロジックの仕様を生成するステップである。このステップ S T 1 3 では、デジタルコンテンツ
20 配布センタ 1 において、実行検証ロジック変換ソフトウェア生成手段 5 によって新たに置き換えられることを意図した第 2 の実行検証ロジックの仕様を実行検証ロジック仕様生成手段 1 1 で生成する。この第 2 の実行検証ロジックの仕様は実行検証ロジックそのものでよいし、異なった形態（例えば形式的言語による記述といったレベルのもの）でも良い。

【 0 0 3 6 】 次のステップ S T 1 4 は、著作権管理代行センタ 1 0 で情報伝達媒体 3 を介して入手したステップ S T 1 3 で生成した第 2 の実行検証ロジックの仕様に基づいて、実行検証ロジック変換ソフトウェア生成手段 5
30 が実行検証ロジック変換ソフトウェアを生成するステップである。このステップ S T 1 4 では、第 2 の実行検証ロジックの仕様が情報伝達媒体 3 を介して著作権管理代行センタ 1 0 へ送られ、実行検証ロジック変換ソフトウェア生成手段 5 は前記第 2 の実行検証ロジックの仕様に基づいて第 2 の実行検証ロジックを伴った実行検証ロジック変換ソフトウェアを生成する。

【 0 0 3 7 】 次のステップ S T 1 5 は、ステップ S T 1 4 で生成した実行検証ロジック変換ソフトウェアの第 2 の実行検証ロジックをデジタルコンテンツ配布センタ 1
40 が情報伝達媒体 3 を介して入手し、実行検証ロジック検証手段 1 2 で検証するステップである。このステップ S T 1 5 では、ステップ S T 1 4 で生成された実行検証ロジック変換ソフトウェアが情報伝達媒体 3 を介してデジタルコンテンツ配布センタ 1 に送られ、そこで得られた実行検証ロジック変換ソフトウェアの第 2 の実行検証ロジックを実行検証ロジック検証手段 1 2 により検証する。この場合の検証内容は、ステップ S T 1 3 で意図した仕様に従った実行検証ロジック（ステップ S T 1 3 で生成した第 2 の実行検証ロジックの仕様と同じ物）へ実
50

行検証ロジック変換ソフトウェアが置き換えを行うことが可能かを判定するものである。

【 0 0 3 8 】 ステップ S T 1 6 は、ステップ S T 1 5 で検証された実行検証ロジック変換ソフトウェアを情報伝達媒体 3 を介して利用者端末 2 に配布するステップである。このステップ S T 1 6 では、前記ステップ S T 1 5 において意図したものとは矛盾しないという判定結果が得られた場合、デジタルコンテンツ配布センタ 1 はステップ S T 1 5 で検証した実行検証ロジック変換ソフトウェアを情報伝達媒体 3 を介して利用者端末 2 に配布する。

【 0 0 3 9 】 ステップ S T 1 7 は、利用者端末 2 において、ステップ S T 1 6 で配布された実行検証ロジック変換ソフトウェアをステップ S T 1 2 で配布されたカプセル化コンテンツ 6 に適用し、カプセル化コンテンツ 6 の第 1 の実行検証ロジック 7 を第 2 の実行検証ロジックに置き換えてインストールするステップである。なお、カプセル化コンテンツ 6 の構造は図 2 に示す前記実施の形態 1 のカプセル化コンテンツと同様である。

【 0 0 4 0 】 また、ステップ S T 1 5 において検証の結果、デジタルコンテンツ配布センタ 1 の意図しない実行検証ロジック変換ソフトウェアが送付された場合、例えば警告メッセージが提示され、それにより利用者への配布を中止し、著作権管理代行センタ 1 0 に異議を唱えるなどの対処ができる。

【 0 0 4 1 】 以上のように、この実施の形態 2 では、著作権管理代行センタ 1 0 が実行検証ロジック変換ソフトウェアの生成を行うので、配布者による配布状況を制作者側が把握できる効果が得られる。また、置き換えるべき実行検証ロジックの仕様の生成と、実行検証ロジック
30 変換ソフトウェアの検証を配布者が行うので、前記実施の形態 1 と同様に配布者が課金に応じて利用者に利用許可を与えることができる効果が得られる。つまり、著作権管理は制作者側で、課金管理は配布者側で、それぞれ行うことができる。

【 0 0 4 2 】 実施の形態 3. 以上、説明した各実施の形態のデジタルコンテンツ配布システム装置では、デジタルコンテンツ配布の全体の流れに着目して説明したが、次に不正使用や改竄に対する安全性をより向上させたデジタルコンテンツ配布システム装置について説明する。
図 6 は、この発明の実施の形態 3 によるデジタルコンテンツ配布システム装置におけるコンテンツカプセル化手段 4 の詳細を示すブロック図である。図 6 において、4 は図 1 において説明したコンテンツカプセル化手段と同様であり、2 1 は第 1 の実行検証ロジックを生成する実行検証ロジック生成手段、2 2 はデジタルコンテンツを暗号化するための共通密鍵（コンテンツ鍵）を生成するコンテンツ鍵生成手段、2 3 はコンテンツ鍵生成手段 2 2 によって生成されたコンテンツ鍵を利用してデジタルコンテンツを暗号化するコンテンツ暗号化手段、2 4 は

電子透かしによりデジタルコンテンツに制作者の指示した著作権などを埋め込む著作権埋込手段（電子透かし組込手段）、25は前記著作権情報の埋め込まれたデジタルコンテンツに対して電子署名を生成する電子署名生成手段、26は実行検証ロジック生成手段21によって生成された第1の実行検証ロジックのメッセージ識別子を生成するメッセージ識別子生成手段（識別子生成手段）、27は電子透かしを施され暗号化されたデジタルコンテンツと電子署名と前記第1の実行検証ロジックとメッセージ識別子を結合するコンテンツ結合手段である。

【0043】図7は、実行検証ロジック変換ソフトウェア生成手段5の詳細を示すブロック図である。図において、実行検証ロジック変換ソフトウェア生成手段5は図1で説明した実行検証ロジック変換ソフトウェア生成手段と同様であり、またメッセージ識別子生成手段26は図6に示したメッセージ識別子生成手段と同様である。28はコンテンツ鍵生成手段22により生成されたコンテンツ鍵を、暗号化を施したデジタルコンテンツのIDと関連付けて管理するコンテンツ鍵管理手段（暗号化コンテンツ管理手段）、29は図4に示した実行検証ロジック仕様生成手段11により生成された第2の実行検証ロジックの仕様に基づいて第2の実行検証ロジックを生成する実行検証ロジック生成手段（第2の実行検証ロジック生成手段）、30は実行検証ロジック生成手段29により生成された第2の実行検証ロジックとメッセージ識別子生成手段26により生成された第2の実行検証ロジックのメッセージ識別子とコンテンツ鍵管理手段28により管理されているコンテンツの共通鍵とを利用して実行検証ロジック変換ソフトウェアを生成する変換ソフトウェア生成手段である。

【0044】図8は、第2の実行検証ロジックの詳細を示すブロック図である。図において、17は図2に示した第1の実行検証ロジックと同様な第2の実行検証ロジックであり、31はカプセル化コンテンツに付加された電子署名の正当性を検証する電子署名検証手段、32はカプセル化コンテンツに付加されたメッセージ識別子の正当性を検証するメッセージ識別子検証手段（識別子検証手段）、33はデジタルコンテンツを暗号化した共通鍵を格納するコンテンツ鍵格納手段（暗号化コンテンツ鍵格納手段）、34はコンテンツ鍵格納手段33にコンテンツ鍵が格納されているか否かを判定するコンテンツ鍵判定手段（コンテンツ鍵格納判定手段）、35は暗号化されたデジタルコンテンツをコンテンツ鍵を利用して復号するコンテンツ復号手段（復号手段）である。

【0045】次に動作について説明する。なお、この実施の形態3では、デジタルコンテンツをカプセル化する動作と実行検証ロジック変換ソフトウェアを生成する動作のみが実施の形態1および実施の形態2と異なるので、異なる部分について説明する。また、以下の説明で

は、実施の形態2と同様の位置にコンテンツカプセル化手段4および実行検証ロジック変換ソフトウェア生成手段5があるものとして説明する。図9は、コンテンツのカプセル化を行う際の動作を示すフローチャートである。ステップST21は、電子透かしによりデジタルコンテンツに著作権情報を埋め込むステップである。このステップST21では、制作者端末9において、まず著作権埋込手段24により、対象となるデジタルコンテンツに適した電子透かし技術により制作者が指示した著作権情報を埋め込む。

【0046】次のステップST22は、デジタルコンテンツを暗号化するためのコンテンツ鍵を生成するステップである。このステップST22では、コンテンツ鍵生成手段22によりカプセル化の対象とするデジタルコンテンツの一部あるいは全部を暗号化するためのコンテンツ鍵を生成する。このとき使用制限や参照制限を施した部分を暗号化の対象とする。

【0047】続くステップST23は、ステップST22で生成したコンテンツ鍵でデジタルコンテンツを暗号化するステップである。このステップST23では、ステップST22でコンテンツ鍵生成手段22により生成したコンテンツ鍵を用いて、コンテンツ暗号化手段23により対象とするデジタルコンテンツを暗号化する。この際、暗号化を施したデジタルコンテンツには識別子を常に参照可能な形で付随させる。

【0048】次のステップST24は、暗号化されたデジタルコンテンツの電子署名を生成するステップである。このステップST24では、電子署名生成手段25により暗号化を施されたデジタルコンテンツの電子署名を生成する。この際、電子署名に用いられる秘密鍵は制作者の秘密鍵とする。

【0049】続くステップST25は、第1の実行検証ロジックを生成するステップである。このステップST25では、実行検証ロジック生成手段21により第1の実行検証ロジック7を生成する。ここで生成される第1の実行検証ロジック7は、図8に示す構造と同様であるが、最初に作成される第1の実行検証ロジック7のコンテンツ格納手段33にはコンテンツ鍵が格納されない。この場合、カプセル化されたコンテンツの起動処理において、暗号化されたデジタルコンテンツは復号されず、その部分は参照も実行もできない。また、コンテンツ格納手段33に、該当するコンテンツ鍵が格納されている場合は、カプセル化されたコンテンツの起動処理において、コンテンツ鍵判定手段34がコンテンツ鍵を検出し、暗号化されていたデジタルコンテンツがコンテンツ復号手段35により復号されて後の処理が進行する。処理進行中は復号されたデジタルコンテンツを利用者端末2の主記憶装置上で保存し、処理終了時には主記憶装置上から復号されたデジタルコンテンツを消去するようにすると、復号されたデジタルコンテンツを容易に取り出

することができなくなり、不正利用や不正な複製に対する安全性が増す。

【0050】次のステップST26は、第1の実行検証ロジックのハッシュ値を取ることによりメッセージ識別子を生成するステップである。このステップST26では、メッセージ識別子生成手段26により第1の実行検証ロジック7のハッシュ値を算出しこれを第1の実行検証ロジック7のメッセージ識別子として生成する。実行検証ロジック生成手段21によって生成された第1の実行検証ロジック7は、自分自身のメッセージ識別子の検証を行うためのメッセージ識別子検証手段32を含むように構成される。

【0051】ステップST27は、暗号化されたデジタルコンテンツ、電子署名、第1の実行検証ロジック、そのメッセージ識別子を結合するステップである。このステップST27では、暗号化されたデジタルコンテンツ、電子署名、第1の検証ロジック7、そして第1の検証ロジック7の前記メッセージ識別子をコンテンツ結合手段27によって結合する。

【0052】次に、実行検証ロジック変換ソフトウェアを生成する動作について説明する。図10は、この実行検証ロジック変換ソフトウェアの生成動作を示すフローチャートである。まず、ステップST31では、デジタルコンテンツ配布センタ1の実行検証ロジック仕様生成手段11により生成された第2の実行検証ロジックの仕様を、情報伝達媒体3を介して実行検証ロジック変換ソフトウェア生成手段5が得る。次のステップST32では、実行検証ロジック変換ソフトウェア生成手段5の実行検証ロジック生成手段29が前記ステップST31で得た第2の実行検証ロジックの仕様について著作権管理代行センタ10にとって許容できるか否かをチェックし、許容できるものであればステップST33以降に処理を進める。この処理を進める場合、ステップST31で得た第2の実行検証ロジックの仕様の内容から暗号化されたデジタルコンテンツの復号が必要であると判明したときには、ステップST33において、暗号化の対象となったデジタルコンテンツのメッセージ識別子をコンテンツ鍵管理手段28に与え、前記デジタルコンテンツを暗号化した共通鍵を得る。

【0053】そして、最後にステップST31で得た第2の実行検証ロジックの仕様から、デジタルコンテンツの著作権情報を検証する電子署名検証手段31、第1の実行検証ロジック7自身の改竄を検証するメッセージ識別子検証手段32、ステップST33で得た共通鍵であるコンテンツ鍵を格納するコンテンツ鍵格納手段33、前記コンテンツ鍵の存在を判定するコンテンツ鍵判定手段34、暗号化されたデジタルコンテンツを復号するコンテンツ復号手段35、コンテンツの使用制限や参照制限などの制御を行うコンテンツ制御手段50、メッセージ識別子生成手段26によって生成された第1の実行検証

ロジック7自体のメッセージ識別子などを含む第2の実行検証ロジック17を生成し、これによってカプセル化コンテンツ6の第1の実行検証ロジック7を置き換える実行検証ロジック変換ソフトウェアをステップST34で生成する。

【0054】以上のように、この実施の形態3によれば、制作者によって指示された著作権情報をデジタルコンテンツに不可分の形で埋め込む著作権情報埋込手段24を提供しているので、デジタルコンテンツの不正使用の抑止を容易に行うことができる効果が得られる。また、デジタルコンテンツを暗号化するコンテンツ鍵生成手段22やコンテンツ暗号化手段23などを提供しているので、デジタルコンテンツの不正利用や不正な複製の防止を容易に行うことができる効果が得られる。また、電子署名を与え、さらに前記電子署名を検証する電子署名生成手段25や電子署名検証手段31を提供しているので、デジタルコンテンツの改竄防止と著作者の確認を容易に行うことができる効果が得られる。また、実行検証ロジックのメッセージ識別子を生成し、さらにメッセージ識別子を検証するメッセージ識別子生成手段26やメッセージ識別子検証手段32を提供しているので、実行検証ロジック自体の改竄防止を容易に行うことができる効果が得られる。

【0055】実施の形態4。前記実施の形態3は、コンテンツ鍵を格納するコンテンツ鍵格納手段33などを含む第2の実行検証ロジックを生成し、これによってカプセル化コンテンツ6の第1の実行検証ロジック7を置き換える実行検証ロジック変換ソフトウェアを生成する構成であり、デジタルコンテンツを暗号化するコンテンツ鍵をそのまま実行検証ロジック変換ソフトウェアに格納するものであったが、この実施の形態4のデジタルコンテンツ配布システム装置は、より安全に前記デジタルコンテンツを暗号化するコンテンツ鍵の授受を行うものである。図11は、この発明の実施の形態4によるデジタルコンテンツ配布システム装置における第2の実行検証ロジック47の構成を示すブロック図である。図11において図8と同一または相当の部分については同一符号を付し説明を省略する。図において、36は利用者の秘密鍵を獲得する秘密鍵獲得手段、37は利用者端末2の利用者の秘密鍵を格納する秘密鍵格納手段である。なお、この実施の形態の実行検証ロジック変換ソフトウェア生成手段5およびコンテンツ鍵格納手段33は暗号化コンテンツ鍵格納手段に対応する。

【0056】次に動作について説明する。なお、この実施の形態4では、実行検証ロジック変換ソフトウェアを生成する動作が前記実施の形態3と異なる。図12は、このデジタルコンテンツ配布システム装置における実行検証ロジック変換ソフトウェアの生成動作を示すフローチャートである。まず、デジタルコンテンツ配布センタ1の実行検証ロジック仕様生成手段11によって生成さ

れた第2の実行検証ロジックの仕様を情報伝達媒体3を介して実行検証ロジック変換ソフトウェア生成手段5が得る。この動作は、図10における実行検証ロジック変換ソフトウェアを生成するステップST31の動作であるが、この実施の形態のステップST41では、デジタルコンテンツ配布センタ1が利用者からのコンテンツ購入要求を得る際に、利用者の公開鍵暗号系における公開鍵を同時に得ておく。続くステップST42では、デジタルコンテンツ配布センタ1から前記公開鍵を前記実行検証ロジックの仕様と共に著作権管理代行センタ10に送付する。

【0057】次のステップST43では、図10のステップST32の処理と同様に、著作権管理代行センタ10の実行検証ロジック変換ソフトウェア生成手段5が前記ステップST42で送付された実行検証ロジックの仕様のチェックを行い、暗号化の対象となったデジタルコンテンツのメッセージ識別子をコンテンツ鍵管理手段28に与え、前記図10のステップST33の処理と同様に、前記デジタルコンテンツを暗号化したコンテンツ鍵を得る。そして最後のステップにおいてコンテンツ鍵格納手段33にコンテンツ鍵を格納する際に、前記ステップST42で送付された利用者の公開鍵によって前記コンテンツ鍵に暗号化を施した上で格納する。また、コンテンツを復号する際には利用者の秘密鍵を獲得する手段である秘密鍵獲得手段36を含めた第2の実行検証ロジック47に置き換えるように、実行検証ロジック変換ソフトウェアが生成される。

【0058】ステップST44からステップST47の処理は、前記実行検証ロジック変換ソフトウェアを生成するための、電子署名、実行検証ロジック、メッセージ識別子などの生成処理およびコンテンツと電子署名、実行検証ロジック、メッセージ識別子との結合処理を示す。

【0059】このような実行検証ロジック変換ソフトウェアを試使用版のカプセル化コンテンツに適用して得られた実使用版のカプセル化コンテンツを利用者が利用する場合、暗号化されたデジタルコンテンツの復号処理は、まず利用者端末2に存在する秘密鍵格納手段37より秘密鍵獲得手段36が利用者の秘密鍵を得て、それを利用してコンテンツ鍵格納手段33に格納されたコンテンツ鍵を復号した上でカプセル化コンテンツの中のデジタルコンテンツの復号が実施される。

【0060】以上のように、この実施の形態4によれば、著作権管理代行センタ10の実行検証ロジック変換ソフトウェア生成手段5がコンテンツ鍵を利用者の公開鍵で暗号化してから実行検証ロジック変換ソフトウェアに含め、利用時には利用者の秘密鍵を利用して前記暗号化されたコンテンツ鍵を復号した上で実際にコンテンツを復号する処理を行うように構成したので、配布者が容易にコンテンツ鍵を取り出すことができない、安全なデ

ジタルコンテンツ配布システム装置が得られる効果がある。

【0061】実施の形態5。この発明の実施の形態5におけるデジタルコンテンツ配布システム装置について説明する。このデジタルコンテンツ配布システム装置では、利用者がカプセル化コンテンツの第1の実行検証ロジックを第2の実行検証ロジックへ置き換えるときに利用者自身の情報を埋め込むことができる。図13は、この発明の実施の形態5によるデジタルコンテンツ配布システム装置における実行検証ロジック変換ソフトウェアの構成を示すブロック図である。図において、38は実行検証ロジック変換ソフトウェア、39はカプセル化コンテンツ6に組み込まれているデジタルコンテンツや第1の実行検証ロジックを検証するカプセル化コンテンツ検証手段、40は新たに置き換える第2の実行検証ロジックを格納する実行検証ロジック格納手段、41は実行検証ロジックを置き換える実行検証ロジック置換手段、42は利用者情報を埋め込む利用者情報埋込手段である。

【0062】次に動作について説明する。図14は、このデジタルコンテンツ配布システム装置における実行検証ロジック変換ソフトウェアを生成する動作を示すフローチャートである。ステップST51は利用者から利用者情報を得るステップである。このステップST51では、利用者がコンテンツの購入を要求するときに、デジタルコンテンツ配布センタ1が利用者によるデジタルコンテンツの購入要求と共に利用者の識別子、氏名、所属などの利用者情報を得る。

【0063】次のステップST52は、ステップST51で得た利用者情報を情報伝達媒体3を介して著作権管理代行センタ10へ送付するステップである。このステップST52では、デジタルコンテンツ配布センタ1から情報伝達媒体3を介して、ステップST51で得られた利用者情報を第2の実行検証ロジックの仕様と共に著作権管理代行センタ10へ送る。

【0064】続くステップST53は、電子透かしにより利用者情報をデジタルコンテンツに埋め込むロジックを持つ実行検証ロジック変換ソフトウェアを生成するステップである。このステップST53では、著作権管理代行センタ10の実行検証ロジック変換ソフトウェア生成手段5により、実行検証ロジック変換ソフトウェアが起動するとその利用者情報をコンテンツに埋め込むような利用者情報埋込手段42を含む実行検証ロジック変換ソフトウェア38を生成する。

【0065】以上のように、この実施の形態5によれば、利用者による購入要求に伴う利用者情報を利用するようにしているので、正確な利用者情報を実行検証ロジック変換ソフトウェアに埋め込むことができる。また、実行検証ロジック変換ソフトウェア38が利用者情報を埋め込む利用者情報埋込手段42を備えるように構成し

ているため、試使用版コンテンツから実使用版コンテンツをインストールする際に、特に煩雑な手間を必要とせず利用者をコンテンツに埋め込むことができる効果が得られる。

【0066】実施の形態6. この発明の実施の形態6におけるデジタルコンテンツ配布システム装置について説明する。この実施の形態6では、カプセル化コンテンツの実行検証ロジックを置き換えるときに課金情報を配布者に伝えることができるデジタルコンテンツ配布システム装置について説明する。図15は、この発明の実施の形態6によるデジタルコンテンツ配布システム装置における実行検証ロジック変換ソフトウェア48の構成を示すブロック図である。図15において図13と同一または相当の部分については同一符号を付し説明を省略する。図において、43は実行検証ロジックの置き換えに際して情報伝達媒体3を介して利用者端末2からデジタルコンテンツ配布センタ1に課金情報を伝達する課金情報提供手段である。

【0067】次に動作について説明する。この実行検証ロジック変換ソフトウェア48の生成は、先ず、デジタルコンテンツ配布センタ1が実行検証ロジック仕様生成手段11により第2の実行検証ロジックの仕様を生成する際、利用者が実行検証ロジック変換ソフトウェア48を起動すると対象コンテンツの識別子、利用者の識別子、名前、所属などを情報伝達媒体3を介してデジタルコンテンツ配布センタ1に送付する仕様にし、このような機能を実現するロジックおよび送付先アドレスを前記第2の実行検証ロジックの仕様に含める。

【0068】次に、この仕様を情報伝達媒体3を介して著作権管理代行センタ10に送付し、著作権管理代行センタ10の実行検証ロジック変換ソフトウェア生成手段5は、前記仕様に基づいて課金情報提供手段43を含む実行検証ロジック変換ソフトウェア48を生成する。

【0069】以上のように、この実施の形態6によれば、実行検証ロジック変換ソフトウェア48の起動時に、予め保持しておいた利用者の識別子、名前、所属などの情報とコンテンツの識別子をデジタルコンテンツ配布センタに送付するようにしているので、コンテンツを試使用版から実使用版へと変換（すなわち実使用版のインストール）する際に課金を行うことができる効果が得られる。

【0070】また、利用者が自由に書き換えることができないようなタンパフリーの領域をデジタルコンテンツ配布センタ1ではなく利用者端末2に設け、前記領域へ格納した利用者の識別子、名前、所属などの情報とコンテンツの識別子を、実行検証ロジック変換ソフトウェア48の起動時に得るように構成することで、実使用版のインストールと課金とを同期させることができる効果が得られる。

【0071】

【発明の効果】以上のように、この発明によれば、使用を許可するための鍵を配布する構成ではなく、第2の実行検証ロジックへ第1の実行検証ロジックを置き換えるように構成したので、予め何を制限するかをデジタルコンテンツに埋め込んでおき、それを実施するか解除するかを実行検証ロジックにより切り換えるだけでなく、前記第2の実行検証ロジックにより後付けでより柔軟な実行の制御をデジタルコンテンツに施すことができる効果がある。

【0072】この発明によれば、実行検証ロジック変換ソフトウェアを著作権管理代行センタで生成するように構成したので、制作者側がデジタルコンテンツの配布の状況を正確に把握できる効果がある。

【0073】この発明によれば、暗号化、電子署名、改竄防止のための手段を組み込むことができるように構成したので、煩雑な手間を要せずに安全性の高いデジタルコンテンツの配布が実現する効果がある。

【0074】この発明によれば、コンテンツ鍵を利用者の公開鍵で暗号化して送付するように構成したので、制作者や利用者以外の者がコンテンツ鍵を参照できないような安全なシステムを提供できる効果がある。

【0075】この発明によれば、実行検証ロジック変換ソフトウェアの実行時に予め得ておいた利用者の情報をデジタルコンテンツ内に埋め込むように構成したので、不正コピーや不正利用の抑止が容易に実現できる効果がある。

【0076】この発明によれば、実行検証ロジック変換ソフトウェアの実行時に課金情報を配布者に送付するように構成したので、デジタルコンテンツや鍵の受け取り否認が抑止しやすくなる効果がある。

【図面の簡単な説明】

【図1】 この発明の実施の形態1によるデジタルコンテンツ配布システム装置の全体構成を示すブロック図である。

【図2】 この発明の実施の形態1によるコンテンツカプセル化手段が生成するデジタル化されたコンテンツを示すブロック図である。

【図3】 この発明の実施の形態1によるデジタルコンテンツ配布システム装置の動作を示すフローチャートである。

【図4】 この発明の実施の形態2によるデジタルコンテンツ配布システム装置の全体構成を示すブロック図である。

【図5】 この発明の実施の形態2によるデジタルコンテンツ配布システム装置の動作を示すフローチャートである。

【図6】 この発明の実施の形態3によるデジタルコンテンツ配布システム装置におけるコンテンツカプセル化手段の構成を示すブロック図である。

【図7】 この発明の実施の形態3によるデジタルコン

テンツ配布システム装置における実行検証ロジック変換ソフトウェア生成手段の構成を示すブロック図である。

【図 8】 この発明の実施の形態 3 によるデジタルコンテンツ配布システム装置における第 2 の実行検証ロジックの構成を示すブロック図である。

【図 9】 この発明の実施の形態 3 によるデジタルコンテンツ配布システム装置におけるコンテンツのカプセル化を行う際の動作を示すフローチャートである。

【図 10】 この発明の実施の形態 3 によるデジタルコンテンツ配布システム装置における実行検証ロジック変換ソフトウェアを生成する動作を示すフローチャートである。

【図 11】 この発明の実施の形態 4 によるデジタルコンテンツ配布システム装置における第 2 の実行検証ロジックの構成を示すブロック図である。

【図 12】 この発明の実施の形態 4 によるデジタルコンテンツ配布システム装置における実行検証ロジック変換ソフトウェアの生成動作を示すフローチャートである。

【図 13】 この発明の実施の形態 5 によるデジタルコンテンツ配布システム装置における実行検証ロジック変換ソフトウェアの構成を示すブロック図である。

【図 14】 この発明の実施の形態 5 によるデジタルコンテンツ配布システム装置における実行検証ロジック変換ソフトウェアを生成する動作を示すフローチャートである。

【図 15】 この発明の実施の形態 6 によるデジタルコ

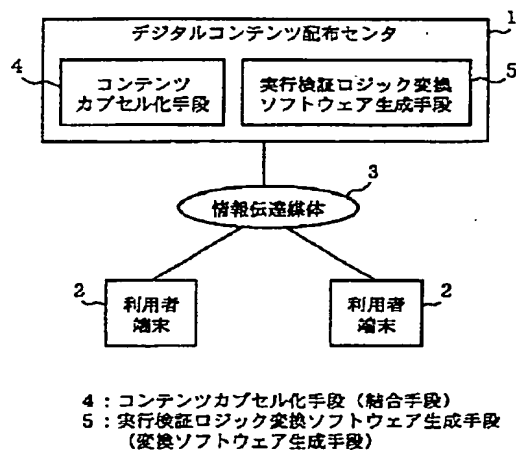
ンテンツ配布システム装置における実行検証ロジック変換ソフトウェアの構成を示すブロック図である。

【図 16】 従来のデジタルコンテンツ配布システム装置の構成を示すブロック図である。

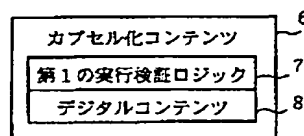
【符号の説明】

1 デジタルコンテンツ配布センタ、2 利用者端末、3 情報伝達媒体、4 コンテンツカプセル化手段（結合手段）、5 実行検証ロジック変換ソフトウェア生成手段（変換ソフトウェア生成手段）、7 第 1 の実行検証ロジック、8 デジタルコンテンツ、9 制作者端末、10 著作権管理代行センタ、11 実行検証ロジック仕様生成手段（仕様生成手段）、12 実行検証ロジック検証手段（比較検証手段）、17、47 第 2 の実行検証ロジック、22 コンテンツ鍵生成手段、23 コンテンツ暗号化手段、24 著作権情報埋込手段（電子透かし組込手段）、25 電子署名生成手段、26 メッセージ識別子生成手段（識別子生成手段）、27 コンテンツ結合手段、28 コンテンツ鍵管理手段（暗号化コンテンツ管理手段）、29 実行検証ロジック生成手段（第 2 の実行検証ロジック生成手段）、31 電子署名検証手段、32 メッセージ識別子検証手段（識別子検証手段）、33 コンテンツ鍵格納手段（暗号化コンテンツ鍵格納手段）、34 コンテンツ鍵判定手段（コンテンツ鍵格納判定手段）、35 コンテンツ復号手段（復号手段）、38、48 実行検証ロジック変換ソフトウェア、42 利用者情報埋込手段、43 課金情報提供手段。

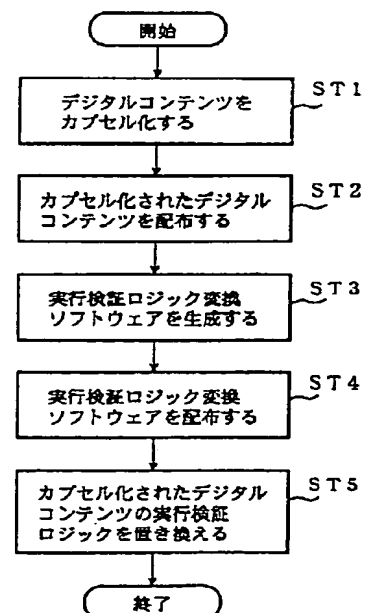
【図 1】



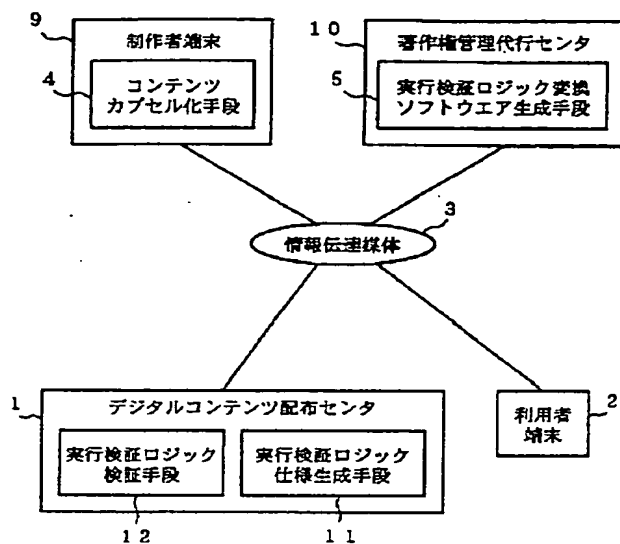
【図 2】



【図 3】

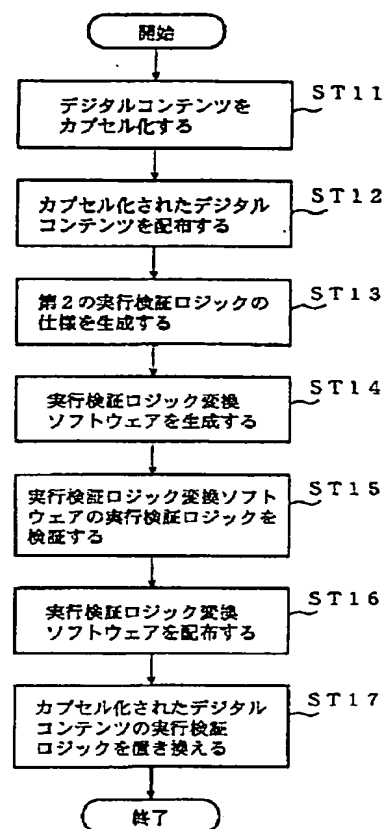


【図 4】

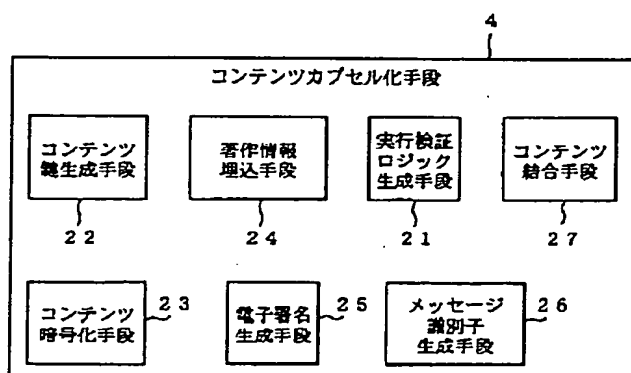


1 1 : 実行検証ロジック仕様生成手段 (仕様生成手段)
 1 2 : 実行検証ロジック検証手段 (比較検証手段)

【図 5】

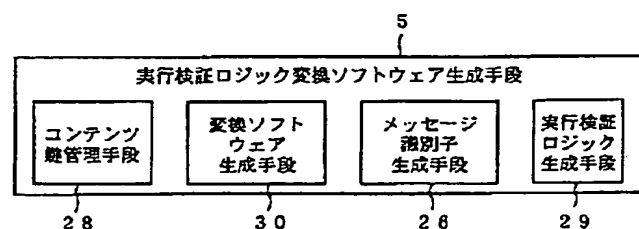


【図 6】



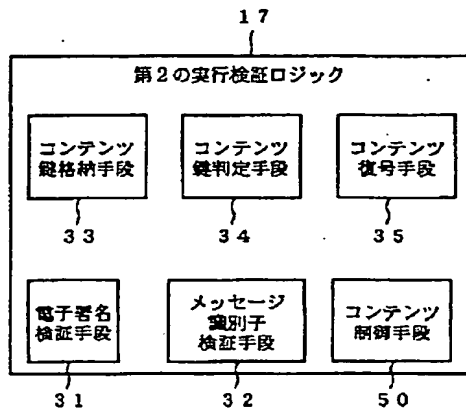
2 4 : 著作権情報埋込手段 (電子透かし埋込手段)
 2 6 : メッセージ識別子生成手段 (識別子生成手段)

【図 7】



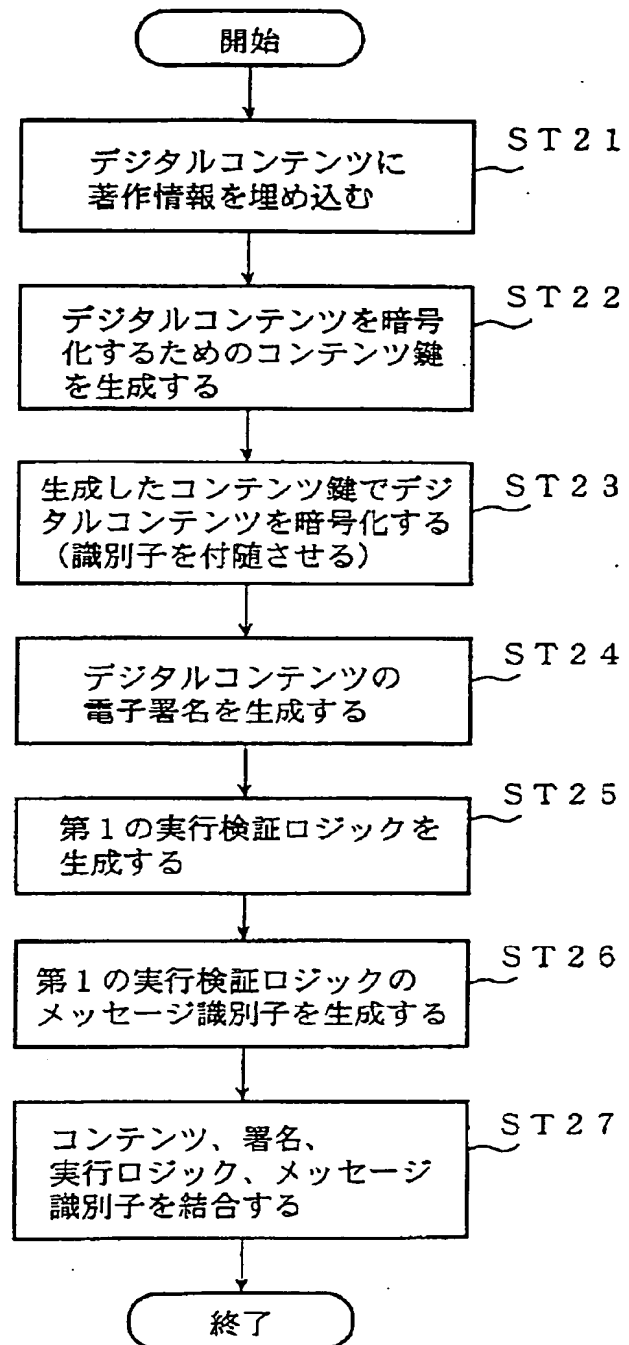
2 8 : コンテンツ暗号管理手段 (暗号化コンテンツ管理手段)
 2 9 : 実行検証ロジック生成手段 (第2の実行検証ロジック生成手段)

【 図 8 】

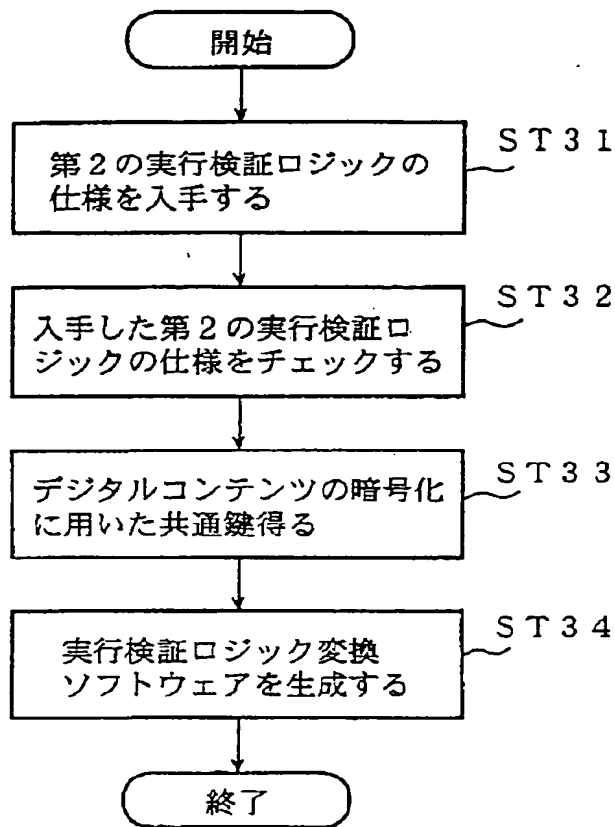


- 32 : メッセージ識別子検証手段 (識別子検証手段)
 33 : コンテンツ鍵格納手段 (暗号化コンテンツ鍵格納手段)
 34 : コンテンツ鍵判定手段 (コンテンツ鍵格納判定手段)
 35 : コンテンツ復号手段 (復号手段)

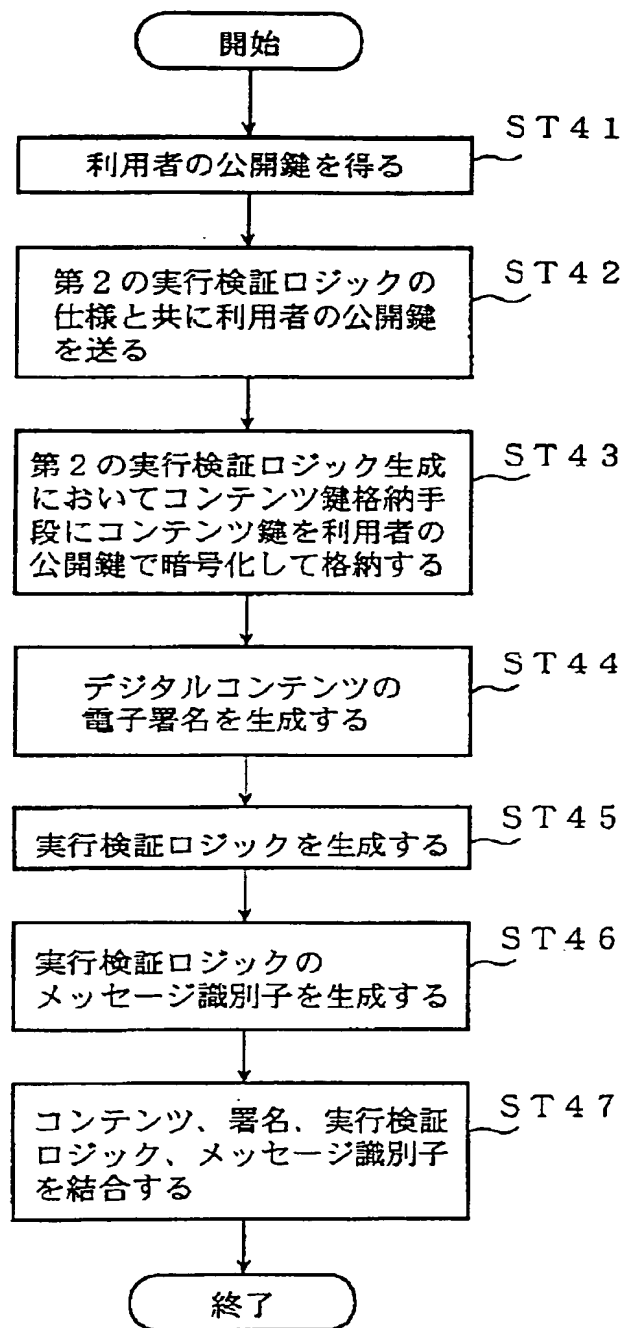
【 図 9 】



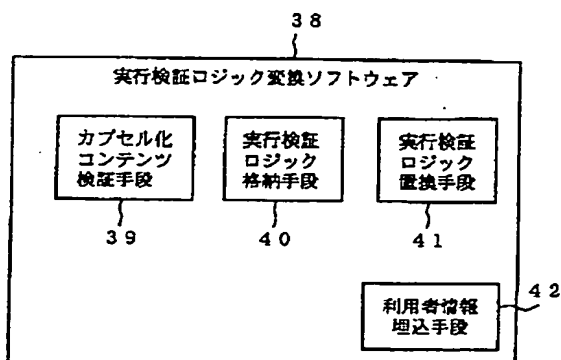
【図 10】



【図 12】

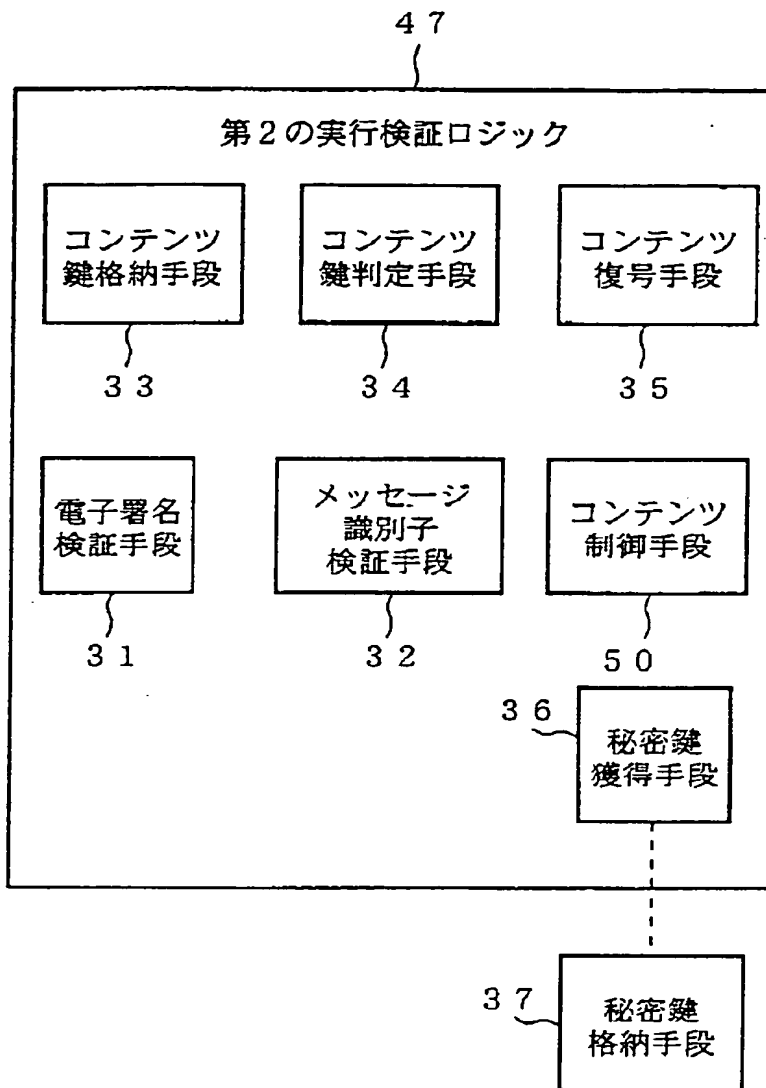


【図 13】

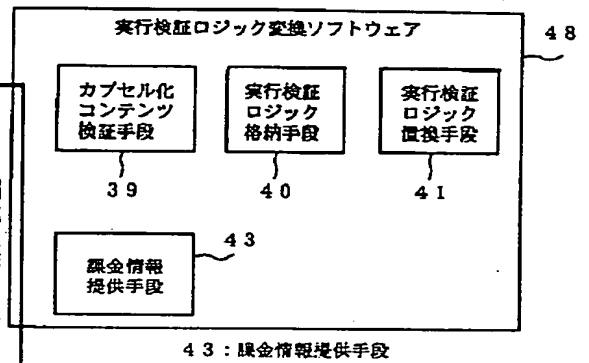


42 : 利用者情報埋込手段

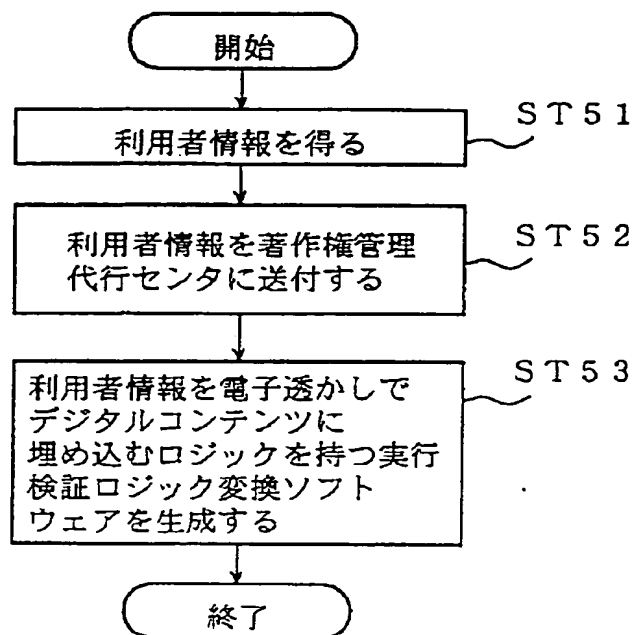
【図 1 1】



【図 1 5】



【図 14】



【図 16】

